基于双线性对的 k-匿名隐私保护方案研究 *

宋 成，张亚东，彭维平，闫玺玺

(河南理工大学 计算机科学与技术学院,焦作 454003)

摘 要：针对移动互联网环境下位置服务的隐私保护问题，基于双线性对性质和 k-匿名的思想，提出了一个高服务质量的隐私增强方案。通过终端在欧几里得距离环形区域内均匀生成 2*k* 个虚假位置，利用位置熵、位置分散度和地图背景信息从中筛选出 *k*-1 个虚假位置，进而达到更优的 k-匿名效果。通过安全性分析，本方案不仅满足隐私性、匿名性、不可伪造性等安全特性，而且能够抗查询服务追踪攻击；仿真实验表明，本方案虚假位置节点选取具有更优的均匀度，同时在假节点生成和选取效率也有所提高。

关键词：基于位置的服务；双线性对；k-匿名；隐私保护

中图分类号：TP309 doi: 10.3969/j.issn.1001-3695.2017.11.0756

Research on k-anonymous privacy protection scheme based on bilinear pairing

Song Cheng, Zhang Ya-dong, Peng Wei-ping, Yan Xi-xi

(*School of Computer Science and Technology Henan Polytechnic University*, *Jiaozuo* 454003, *China*)

Abstract: Aiming at the privacy protection problem of location service in mobile Internet environment, a high quality of service privacy enhancement scheme based on bilinear pairing property and anonymity is proposed. The terminal generates 2*k* evenly distributed false locations in the ring area of Euclidean distance. According to location entropy, location dispersion and map background information, the terminal screens superior *k*-1 false locations from them to achieve better k-anonymity. Through the security analysis, the scheme not only satisfies the privacy, anonymity, unforgeability etc. , but also can resist query service tracking attack. The simulation experiments show that the selection of false position nodes in this scheme has a better uniformity, and the efficiency of the false node generation and selection is also improved.

Key words: location-based services; bilinear pairings; k-anonymity; privacy protection

0 引言

随着移动通信技术、定位技术及智能设备的迅猛发展，基于位置的服务[1~3]（LBS）得到广泛的应用，越来越多的人受益于相关服务[4]。LBS 应用服务系统已经涉及到各种领域，例如医疗，交通，社交网络、大众娱乐等。然而，基于位置的服务在为用户提供服务的同时，用户敏感数据信息可能被搜集，从而推测出用户个人隐私。如：用户位置信息统计，可推断出用户的家庭和单位地址；结合地图相关信息，可以推断出用户的健康状况，生活习惯和宗教信仰[5]。 因此，位置服务中的用户隐私保护一直是国内外学者关注的焦点[6~8]。

然而，在用户隐私保护技术中，*k*-匿名[9]是重要的技术之一，可以有效防止隐私的泄露，因此 K _匿名技术亦成为目前研究的热点。基于 *k*-匿名的用户的隐私保护方案是由 KIDO[10]等人在 2005 年首次提出。基本思想是：为用户生成多个虚假位置，然后将所选虚假位置和用户的真实位置一起发送到 LBS 服务器。以致攻击者和服务器均无法辨别用户的真实位置。LU 等人在方案[11]中指出，如果虚假位置太过于集中，会降低用户的隐私保护程度，并提出了新的方案，将每个虚假位置均匀位于不同的圆形或矩形区域内，进而提高用户隐私保护程度。NIU 等人[12]指出，上述方案均未考虑攻击者是否知晓背景信息，此信息会影响攻击者对用户的实际位置的推断概率。因此，他们提出一个新的解决方案：生成尽可能多地虚假位置，这些虚假位置与用户真实位置具有相同查询频率，从而加强用户的隐私保护。但该方案不适用于连续 LBS 服务请求查询，因为攻击者根据相邻查询时间和空间之间的联系，可以推断出用户的真实位置。

XU 等人在文献[13]中通过在最小边界圆中选择不包含前

基金项目：国家自然科学基金青年基金项目（61300124，61300216）；河南省科技攻关计划（132102210123）

作者简介：宋成，(1980-）男，河南信阳人，博士，河南理工大学计算机科学与技术学院，讲师，硕导，主要研究方向为网络信息安全、密码学、物联网安全等（songcheng@hpu.edu.cn.）；张亚东，男，通信作者，河南驻马店人，河南理工大学研究生，主要研究方向为物联网安全，隐私保护等；彭维平，男，湖北天门人，博士，河南理工大学副教授，主要研究方向为物联网安全及应用、数据防泄露等；闫玺玺，女，河南灵宝人，博士，河南理工大学讲师，主要研究方向为数字版权管理、数字内容安全、计算机网络安全.

一匿名区内所有其他用户的方法来生成匿名集合，并根据匿名集合大小来衡量用户位置隐私保护的强度。在文献[14]中，提出一个基于用户感觉的连续 LBS 服务请求的隐私保护模型，让用户根据隐私保护的程度构建公共区域。但这两个方案均不能抵抗查询跟踪攻击。WANG 等人在文献[15]中指出在连续的位置服务请求中，用户可能在不同位置隐私保护级别不同，提出一个位置感知的位置隐私保护方案。LI 等[16]指出，如果使用其他用户的历史足迹构建匿名区域，会造成匿名区域太大，进而降低服务质量。提出一个连续 LSB 请求环境下的需求感知位置隐私保护方案，通过删除最远的足迹缩小匿名区域范围，提高服务质量。但是，在用户预定/预测位置之外进行服务请求，该方案仍不能抵抗查询跟踪攻击。SCHLEGEL 等人[17]基于密文匹配思想，提出了基于密文的位置隐私保护方案，在确保第三方可信的情况下，可以抵抗查询跟踪攻击。针对以上不足之处，本文结合双线性对理论知识和 *k*-匿名的思想，提出了一个安全加强的用户位置隐私保护的方案，通过移动终端在欧几里得距离环形区域内均匀生成 $2k$ 个虚假位置，然后利用位置熵、位置分散度和地图背景信息从 $2k$ 个虚假位置中筛选出 $k-1$ 个更优的虚假位置，进一步提高虚假位置均匀度，进而达到更优的 *k*-匿名效果。

1　预备知识

1.1　位置隐私保护系统结构

本文在 *k*-匿名思想的基础上，增加了一个混淆服务器，如下图 1 所示，系统主要由三部分实体组成：移动终端、混淆服务器、位置信息服务器。各部分的作用如下：

移动终端：移动终端具有两个的作用，一是向混淆服务器发送用户假名生成请求并验证假名结果的有效性；二是生成并筛选虚假位置节点，向位置信息服务器发送位置查询请求，并接收来自位置信息服务器的查询结果。

混淆服务器：在匿名位置隐私保护中，通常需要配置一个混淆服务器，为移动终端用户生成假名并将结果发送给移动终端。

位置信息服务器：是位置隐私保护系统的核心部分，负责处理来自移动终端的匿名化查询；并将查询结果返回给移动终端。

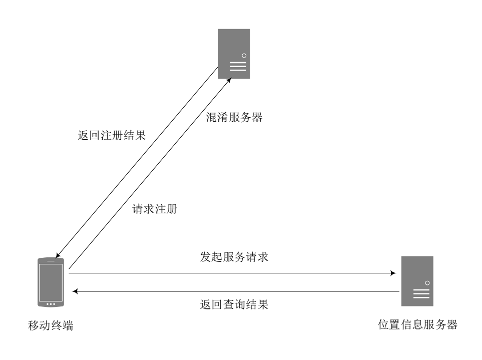


图 1　位置隐私保护系统模型

1.2　双线性对

设 $(G_1,+)$ 为阶为素数 q 的加法循环群，$(G_2,\times)$ 为阶为素数 q 乘法循环群，P 为 G_1 的生成元。双线性映射 $e:G_1\times G_1\to G_2$ 满足以下性质：

（1）双线性：对于：

$$\forall a,b\in Z_q^*,P,Q\in G_1,e(aP,bQ)=e(P,Q)^{ab}$$ ；

（2）非退化性：$\exists P,Q\in G_1$ ，满足 $e(P,Q)\neq 1$ ；

（3）可计算性：对于任意 $P,Q\in G_1$ ，存在有效的算法计算 $e(P,Q)$ ；

1.3　位置熵

给定一个包含 k 个虚假位置的匿名区域，用户在某一虚假位置 i 的概率是 Y_i，那么它的位置熵值为：

$$Y_i \tag{1}$$

在移动终端用户向 LBS 服务器进行服务请求过程中，隐私级别通过单个用户隐私度量标准来衡量。假设匿名区域内 k 个候选虚假位置节点，k 个虚假位置的查询概率分别为 $W_i(i=1,2\cdots k)$，那么每个位置成为真实位置的概率为：

$$2K \tag{2}$$

因此，利用式（1）和（2）可计算出节点位置熵，即攻击者推导出真实位置的信息量。候选位置节点熵值越高，隐私保护水平越高。显然，当所有的 Y_i 相等时，位置节点位置熵值最大，隐私保护水平最高。

1.4　位置分散度

若存在多个虚假位置节点集合中的节点位置熵相等且均是最大值时，将需要利用位置分散度对它们再次进行筛选。因为虚假位置节点集合的位置分散度越大，则表明其所形成的区域面积就越大，这样可以避免由于生成的假节点过于集中，导致攻击者能够推测出用户真实位置所在的区域而造成位置隐私泄露。通常采用虚假位置节点对之间的距离之积来衡量位置分散度。

如图 2 所示，假设 o 是用户的真实位置，p 为已选出的虚拟位置，通过构造椭圆从两个候选位置 m 和 n 中选择出第三个虚拟位置。将 o 和 p 作为椭圆的两个焦点，并将 m 和 n 构造到椭圆上。因为 $mo+mp=no+np$，无法根据虚拟节点对之间的距离之和确定选择哪个节点，但由于 $mo\times mp>no\times np$，最终选择节点 m 作为虚拟位置而不是节点 n，因为节点 m 的分散度更大。

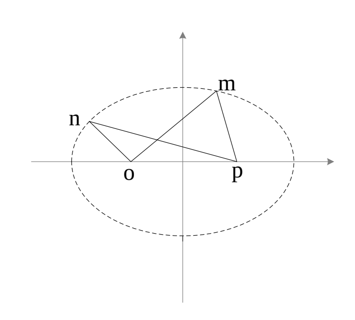


图 2　候选节点筛选示意图

2　基于双线性对的 K-匿名隐私增强方案

本方案主要包括四个阶段：系统初始化阶段、用户注册阶段、假位置生成与选取阶段和位置服务请求阶段。

2.1　系统初始化

系统初始化阶段主要生成系统参数，具体步骤如下：

Step1：G_1，G_2 是两个阶数为素数 q 的循环群，其中 G_1 为加法循环群，G_2 为乘法循环群，P 是 G_1 的生成元。$e:G_1\times G_1\rightarrow G_2$ 表示一个双线性映射。Z_p^* 表示模 q 的整数乘法群。

Step2：定义 2 个安全哈希函数 H_1，H_2 和一个基于椭圆曲线密码体制的加密函数 $enc()$。其中 $H_1:\{0,1\}^*\rightarrow\{0,1\}^k$，$H_2:\{0,1\}^*\rightarrow G_1$，$\{0,1\}^*$ 表示任意长度的二进制串。

Step3：混淆服务器选取系统主密钥 $s\in Z_p^*$，计算其公共密钥为：$P_A=sP$。

Step4：混淆服务器保存系统主密钥 s，公开系统参数：

$$\{G_1,G_2,e,k,P,P_A,H_1,H_2,enc()\}。$$

2.2　用户注册

由于本方案是基于 k-匿名思想而设计的，因此，用户注册阶段，通过混淆服务器对用户的身份进行匿名化，具体步骤如下：

Step1：用户 $User$ 随机选择一个秘密值 $r_u\in Z_p^*$，并将 r_u 和用户真实身份 ID 作为注册请求消息发送给混淆服务器，请求注册。

Step2：混淆服务器收到注册请求后，为用户计算虚假身份：$PID_u=enc(H_1(ID\,||\,r_u))$，然后计算 $Q_u=H_2(PID_u,r_uP)$，$X_u=sQ_u$，并将 $\{PID_u,X_u\}$ 返回给用户 $User$。

Step3：用户 $User$ 收到消息 $\{PID_u,X_u\}$ 后，计算 $\tilde{Q}_u=H_2(PID_u,r_uP)$ 并判断 $e(X_u,P)\overset{?}{=}e(\tilde{Q}_u,P_A)$ 是否成立。如果等式成立，注册成功；否则，返回 Step1 重新注册。

2.3　假位置生成与选取

本阶段通过用户移动终端生成虚假位置，并从 $2k$ 个虚假位置中选取最优的 $k-1$ 个位置，具体步骤如下：

Step1：移动用户终端以用户 $User$ 的真实位置 Loc_{User} 为中心点，采用矩形区域内均匀分布随机点算法生成一个假位置 Loc_i，根据地图的背景信息判断该位置，若为山川、河流等位置，则放弃该位置从新生成；否则，计算 Loc_{User} 和 Loc_i 两位置之间的欧几里得距离：$dis(Loc_{User},Loc_i)$。

Step2：移动用户终端判断不等式 $R_{\min}<dis(Loc_{User},Loc_i)<R_{\max}$ 是否成立。如果满足，让 $c_i=Loc_i$，并将其加入位置集合 $C=\{c_1,c_2,c_3,......,c_{i-1}\}$，即 $C=\{c_1,c_2,c_3,......,c_{i-1}\}\cup\{c_i\}$；如果不满足，重新返回 Step1。其中 $R_{\min}$ 和 $R_{\max}$ 分别表示中心点到新生成假节点的最短距离和最长距离。

Step3：若 $i<2k$，$i=i+1$，并返回 Step1；若 $i=2k$，则执行下一步。

Step4：假设假位置节点集合 C 内假位置的查询概率分别为 $W_i(i=1,2\cdots 2k)$，根据式（2）计算出每个假节点位置成为真实节点位置概率 Y_i。Y_i 越接近真实位置 Loc_{User} 的查询概率，位置熵 $H(x)$ 越高，隐私保护水平就越高。根据该原则，从 $2k$ 个假位置中选取最优的 $k-1$ 个假位置{ $Loc_1,Loc_2\cdots Loc_{k-1}$ }。

注：　Step4 中若在临界位置存在并列无法排除的假节点，即若出现候选假位置 Loc_{k-1} 和 Loc_k 成为真实节点位置概率 Y_{i-1} 和 Y_i 相等的情况，移动终端根据位置分散度原则，判断不等式

$$dis(Loc_{User},Loc_{k-1})\times dis(Loc_p,Loc_{k-1})\overset{?}{>} dis(Loc_{User},Loc_k)\times dis(Loc_p,Loc_k)$$

是否成立　，若成立，则选择 Loc_{k-1} 为候选位置，反之选择 Loc_k 为候选位置，其中 Loc_{User} 为用户 $User$ 的位置，Loc_p 为已选的假位置。最终选择最优的假位置集合 $C_{End}=\{c_1,c_2,c_3,......,c_{k-1}\}$。

Step5：最优的假位置集合 C_{End} 内各位置节点分别进行用户注册，为每个假位置分别生成匿名用户 ID：PID_i（$0<i\le k-1$）。

2.4　位置服务请求

本阶段通过移动终端 $User$ 随机选取一位置节点作为代表节点向 LBS 服务器发送服务请求，具体的请求步骤如下：

Step1：用户从包括真实位置节点在内的 k 个位置节点中随机选取一位置节点 c_j（$0<j\le k$）。

Step2：聚合 k 个节点的假身份 PID_i、节点位置 Loc_i 以及查询内容 Q_i，形成一个查询集合：$\{Msg\{(PID_1,Loc_1,Q_1),(PID_2,Loc_2,Q_2).......,(PID_k,Loc_k,Q_k)\}\}$，以 c_j 位置为代表向 LBS 服务器发送服务请求。

Step3：LBS 服务器接收到服务请求后，将查询结果集 $Rs=\{rs_1,rs_2,rs_3,.......,rs_k\}$ 返回给用户　。

Step4：用户收到 Rs 后，从中选取出用户需求的真实信息 rs_{User}。

3　安全性分析

方案从隐私保护、匿名性、不可伪造性和查询服务跟踪四个方面进行安全性分析。

3.1　隐私保护

本方案通过设置最大半径和最小半径，并且限制最小半径的约束条件。同时再加上虚拟节点的产生是均匀的，在请求位置服务是时随机选取一个节点作为代表节点进行服务请求。这样即使攻击着获取了请求服务的信息也无法得知真实用户位置的信息。在用户注册阶段，所有用户都通过加密算法 $enc()$ 对其节点真实身份 ID 进行加密形成虚假身份 $PID_u=enc(H_1(ID\,||\,r_u))$，攻击者无法从 PID_u 推导或获取节点的真实信息，从而保护了用户信息隐私。在服务请求阶段由于随机选取一个节点作为代表节点发送服务请求。具有随机性，降级攻击者辨别出到底哪个是真实用户的查询信息的概率。进而

保护了真实用户查询信息的安全。

3.2 匿名性

本方案在用户注册阶段，通过加密算法 $enc()$ 对所有节点真实身份 ID 进行加密形成虚假身份 $PID_u=enc(H_1(ID\|r_u))$，攻击者无法从 PID_u 推导或获取节点的真实信息，实现匿名的效果。同时在虚假位置的生成和选取阶段，基于 $K-$匿名的思想，采用匿名区域内均匀分布随机点算法在欧几里得距离环形区间内选取 $2K$ 个虚假节点，然后根据位置熵与位置分散度的原则从 $2k$ 个虚假节点内选取最优的 $k-1$ 个虚假节点，实现混淆的效果。在服务请求阶段，用户从 k 个节点中随机选择一个节点作为代表元素向 LBS 服务器发送服务请求，攻击者即使获得请求数据包，也无法确认信息是否来自真实节点，进一步增强了用户匿名效果。

3.3 不可伪造性

在基于求解椭圆曲线离散对数难题及混淆服务器的前提下，攻击者无法冒充混淆服务器伪造用户注册信息。在用户注册阶段，混淆服务器为用户的真实身份进行加密生成可验证性的假身份 PID_u，混淆服务器返回给注册用户信息 $\{PID_u,X_u\}$ 后，用户需要计算 $\tilde{Q}_u=H_2(PID_u,r_uP)$ 并判断等式 $e(X_u,P)\overset{?}{=}e(\tilde{Q}_u,P_A)$ 是否成立。若攻击者冒充混淆服务器伪造用户注册信息， 在没有获得混淆服务器私钥 s 的情况下，该等式无法成立。如果攻击者设法获取混淆服务器私钥 s，需要利用混淆服务器公钥信息 (P,P_A)，通过 $P_A=sP$ 推导私钥 s，即面临求解椭圆曲线离散对数难题。

3.4 抵抗查询追踪攻击

查询追踪攻击也称为连续查询攻击，其原理是攻击者根据不同时刻某一用户发出的连续查询，获取不同时刻内匿名区域包含的用户集，通过计算不同匿名区域的用户集的交集推断出发出查询的用户。在本方案中由于所选虚假节点均是均匀产生的，而且根据位置熵、位置分散度以及地图背景信息等原则，所选虚假节点与真实节点相似度高，形成的匿名区域面积大，有效抵制查询追踪攻击。而且每次发出 LBS 服务请求都会从 k 个位置节点中随机选取某一个元素作为代表元素发出请求信息，攻击者更无法通过用户连续查询请求节点的交集获取真实节点。

通过以上分析，本方案与相关文献方案的安全分析比较结果如表 1 所示。

表 1 安全性比较

方案	文献[6]	文献[7]	文献[8]	本文方案
位置隐私	√	√	√	√
查询隐私		√	√	√
用户信息隐私				√
匿名性	√	√	√	√
不可伪造性				√
查询追踪攻击				√

4 仿真实验

本文仿真实验环境为：CPU：Intel i5 处理器， 内存：8G。操作系统： Windows7 64 位，仿真软件：MATLAB 软件。假设在一个具有理想的网络环境进行仿真实验。本实验将随机选择一个节点作为用户的真实位置，然后从符合用户需求的虚假位置生成效率和位置分布均匀度两个方面进行仿真。

虚假位置生成算法性能指标主要体现在效率和位置均匀度。相同的实验环境下，通过对比传统方案、CirDummy 方案和 GirdDummy 方案得出以下结论。如图 3 所示，生成符合用户条件虚假位置所需要的时间与匿名度 k 成线性关系，随着匿名度 K 的增加，生成符合用户条件虚假位置生成所需时间也在逐步增加。这是由于随着匿名度 k 的增加，生成的虚假位置数量也随着增多，需要判断的符合用户需求虚假位置个数增加，进而生成时间相应增加。通过仿真实验发现，当 $k\le5$ 时，本方案所生成的符合条件的虚假位置的效率与传统方案算法效率接近；当 $k>5$ 时，本文方案所生成的符合条件的虚假位置的效率与传统方案相比，优势越来越明显，由于传统方案算法生成虚假位置在顺时针旋转的夹角 θ 内，既满足 $\theta=2\pi/(k-1)$，随着匿名度 k 的增加，夹角 θ 越来越小，虚假位置生成在 θ 内的概率越来越小。因此，传统方案生成符合条件的虚假位置算法随着匿名度 k 的增加效率越来越明显低于本文方案。同时对比 CirDummy 方案和 GirdDummy 方案，随着匿名度 k 的增加，本文方案的效率也是越来越高于 CirDummy 方案和 GirdDummy 方案。

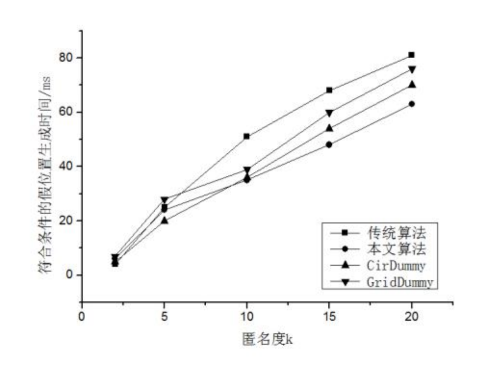


图 3 匿名度 k 与所选位置生成时间的关系

位置的均匀度代表所选的位置与真实位置越相似程度，其均匀程度越高，虚假节点分布越均匀，攻击者找到真实位置的几率越小。位置分布均匀度用 $V=f/k$ 表示，其中 f 表示包含真实位置和虚假位置的最小矩形区域面积， k 表示匿名度。显然，在 f 一定的情况下，位置均匀度随着匿名度 k 的增加而降低。本仿真实验是在最小区域半径为 0.1km，最大区域半径为 0.15km 内进行位置的选择。本方案通过与传统方案和 CirDummy 方案在同等环境下仿真对比结果如图 4 所示，由于本方案采用位置熵、位置分散度和地图背景信息筛选每个虚假位置，因此，本方案位置分布均匀度始终优于传统生成算法，

避免了因位置节点分布集中而导致匿名区域面积缩小的情况，进而增加了攻击者确定用户的真实位置的难度。在位置均匀度仿真实验中之所以没有与 GirdDummy 方案进行对比分析是因为本文实验是在环形区域选取虚假节点，而 GirdDummy 方案与之不符合。

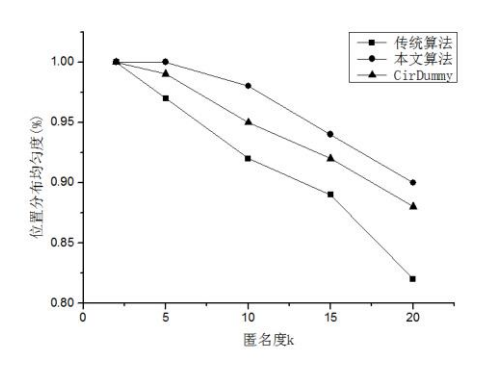


图 4　匿名度 k 与位置分布分均匀度的关系

5　结束语

本文针对移动互联网中用户使用 LBS 服务的位置隐私保护问题，结合双线性对理论知识和 *k*-匿名的思想，提出了一个安全加强的用户位置隐私保护的方案。方案通过移动终端在欧几里得距离环形区域内均匀生成 $2k$ 个虚假位置，然后利用位置熵、位置分散度和地图背景信息从 $2k$ 个虚假位置中筛选出 $k-1$ 个更优的虚假位置。通过安全性分析，本方案解决隐私性、匿名性、不可伪造性以及查询攻击等相关安全问题，安全性得到有效增强；通过仿真实验分析，当 $k\le5$ 时，本方案所生成的符合条件的虚假位置的效率与传统方案算法效率接近；当 $k>5$ 时，具有更高的效率，同时方案具有更高的虚假位置均匀度，从而进一步的提高了用户隐私的保护程度。因此本方案在资源受限的移动互联网或物联网环境中 LBS 位置隐私保护领域有着重要的理论研究意义和应用价值。

参考文献：

[1] Tiwari S, Kaushik S, Jagwani P, et al. A Survey on LBS: System Architecture, Trends and Broad Research Areas [M]// Databases in Networked Information Systems. Springer Berlin Heidelberg, 2011: 223-241.

[2] Krumm, John. A survey of computational location privacy [J]. Personal and Ubiquitous Computing, 2009, 13 (6): 391-399.

[3] Sun Yanming, Chen Min, Hu Long, et al. ASA: Against statistical attacks for privacy-aware users in Location Based Service [J]. Future Generation Computer Systems, 2016, 70.

[4] Xin Mingjun, Lu Manli, Li Wweimin. An adaptive collaboration evaluation model and its algorithm oriented to multi-domain location-based services [J]. Expert Systems with Applications, 2015, 42 (5): 2798-2807.

[5] 万盛，李凤华，牛犇等. 位置隐私保护技术研究进展 [J]. 通信学报. 2016, 37 (12): 125.

[6] Talukder N, Ahamed S I. Preventing multi-query attack in location-based services [C]// ACM Conference on Wireless Network Security. ACM, 2010: 25-36.

[7] Gao Sheng, Ma Jianfeng, Shi Weisong, et al. TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing [J]. IEEE Transactions on Information Forensics & Security, 2013, 8 (6): 874-887.

[8] Mascetti S, Freni D, Bettini C, et al. Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies [J]. The international Journal on Very Large Data Bases, 2011, 20 (4): 541-566.

[9] Liu Xinxin, Liu Kaikai, Guo Linke, et al. A game-theoretic approach for achieving k-anonymity in Location Based Services [C]// INFOCOM, 2013 Proceedings IEEE. IEEE, 2013: 2985-2993.

[10] Kido H, Yanagisawa Y, Satoh T. Protection of Location Privacy using Dummies for Location-based Services [C]// International Conference on Data Engineering Workshops. IEEE Computer Society, 2005: 1248.

[11] Lu Hua, Jensen CS, Man LY. PAD: privacy-area aware, dummy-based location privacy in mobile services [C]// ACM International Workshop on Data Engineering for Wireless and Mobile Access, Mobide 2008, June 13, 2008, Vancouver, British Columbia, Canada, Proceedings. DBLP, 2008: 16-23.

[12] Niu Ben, Li Qinghua, Zhu Xiaoyan, et al. Achieving k-anonymity in privacy-aware location-based services [C]// IEEE INFOCOM. IEEE, 2014: 754-762.

[13] Xu T, Cai Ying. Exploring Historical Location Data for Anonymity Preservation in Location-Based Services [C]// INFOCOM 2008. the, Conference on Computer Communications. IEEE. IEEE, 2008: 547-555.

[14] Xu T, Cai Ying. Feeling-based location privacy protection for location-based services [C]// ACM Conference on Computer and Communications Security. ACM, 2009: 348-357.

[15] Wang Yu, Xu Dingbang, He Xiao, et al. L2P2: Location-aware location privacy protection for location-based services [C]// INFOCOM, 2012 Proceedings IEEE. IEEE, 2012: 1996-2004.

[16] Li Xinghua, Wang Ermeng, Yang Weidong, et al. DALP: A demand-aware location privacy protection scheme in continuous location-based services [J]. Concurrency & Computation Practice & Experience, 2016, 28 (4): 1219-1236.

[17] Schlegel R, Chow C Y, Huang Q, et al. User-Defined Privacy Grid System for Continuous Location-Based Services [J]. IEEE Transactions on Mobile Computing, 2015, 14 (10): 2158-2172.